ƒ 4,-

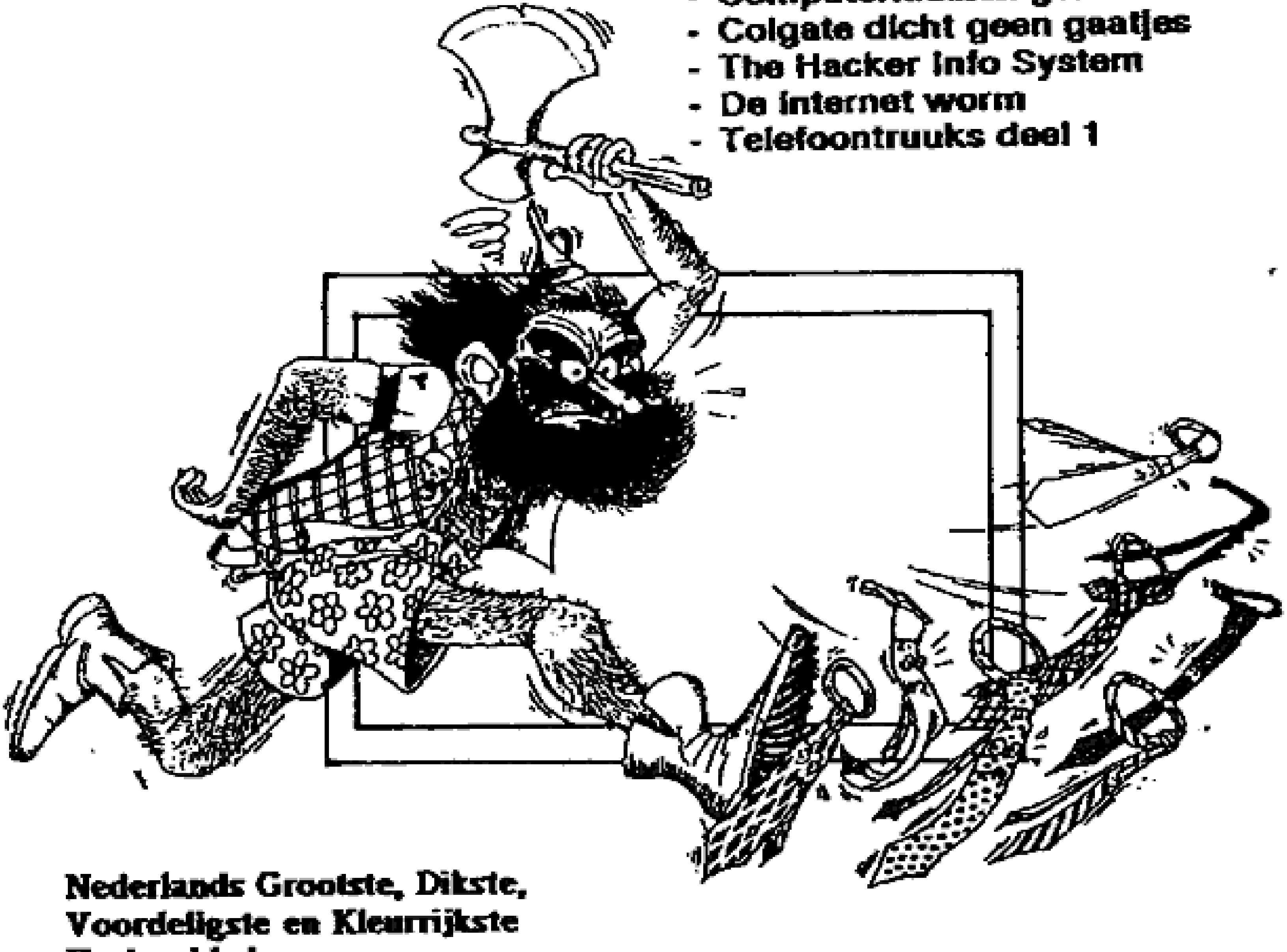
HACK-TIC

NO. 1

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

Met in dit eerste nummer:

- Computerkluizen gekraakt
- Colgate dicht geen gaatjes
- The Hacker Info System
- De internet worm
- Telefoontruuks deel 1



Nederlands Grootste, Dikste, Voordeligste en Kleurrijkste Hacker-blad

COLOFON

HACK-TIC: is Nederlands eerste hackerblad. Naar we hopen verschijnt het ongeveer 10 x per jaar.
UITGAVE: met moeite (door een volkomen ongebonden en ongeorganiseerd gezelschap van vreemde types).
REDAKTIE: The Key, John D., Tx, Herman Acker, Peter Poelman en Rop.
ILLUSTRATIES: Koen Hottentot.
KONTAKT: De redaktie is te bereiken via **p.b. 22953, 1100 DL Amsterdam.** Op UUCP als **..!mcvax!neabbs!rop.** Op het FIDO net **2:280/1 Hack Tic.** Telex (modem 50 baud telecommunicatiecomfort van de PTT) **12969 neabs nl**, telefax **020-763706.** Zowel bij telex als bij fax even vermelden dat het voor Hack-Tic is. Abonnees die er in slagen de redaktie telefonisch (voice) te bereiken moeten met sancties rekening houden.
PRIJS: Losse nummers kosten 4 gulden, een abonnement voor 10 nummers (moet ongeveer een jaar meegaan) kost ƒ 37.50. Abonnementsgelden overmaken op bankrekeningnummer **98.72.84.541** t.n.v. Rop Gonggrijp.
PRIVACY: Het is waar: als 'ze' willen, hoeven ze alleen maar naar onze bankafschriften te kijken om te zien wie er abonnee zijn. Wij vinden Hack-Tic een uiterst onschuldig blaadje, maar de kans bestaat dat lokale, regionale, nationale en in de toekomst wellicht zelfs Europese overheden het daar niet mee eens zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres bijsluiten in een envelop en die aan onze postbus sturen, wij weten dan genoeg (jaja, als ze de post open maken ben je nog steeds de pisang). De Hack-Tic wordt altijd verstuurd in een neutrale envelop. (Straks denkt je hospita nog dat je porno koopt per postorder). Hack-Tic is ook verkrijgbaar bij de goede boekhandel (wellicht herkenbaar aan het observatieteam voor de deur).

DISCLAIMER: Informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af.

HOE: Hack-Tic werd met het WYSMRWYG (What You See Might Resemble What You Get) DTP pakket Ventura 1.1 gemaakt op een gammele AT. Print-outs van elke pagina gemaakt met een EPSON RX-80 en daarna verkleind en gefotokopieerd. Dan nog een nietje d'r in en klaar was Kees (hopen we terwijl we dit tikken).

IN DIT NUMMER:

Hackers beginnen Nederlands eerste kritische computerblad.

Hack-Tic is een nieuw maandblad voor hackers. Het bevat alle truuks en tips die andere bladen niet hebben. Nieuws over Computer-Hacking, Phone-Phreaking of andere vormen van techno-anarchisme vindt je altijd eerst in Hack-Tic.

Maar ook achtergrondverhalen over informatisering(sblunders), grote computernetwerken en de overmatige opslag van privacy gevoelige gegevens komen aan bod. Zodoende is Hack-Tic interessant voor iedereen die zich kritisch opstelt ten opzichte van de informatiemaatschappij.

Big Brother

Want Big Brother kijkt steeds vaker mee, al doet hij dat in onschuldig lijkende vermommingen. Het gerucht doet de ronde dat hij zich in Nederland heeft vermomd als giromaat. Ook zou hij de man achter de schermen zijn bij het road-pricing plan van minister Smit-Kroes. Vaak is hij echter minder subtiel. Op zijn orders worden in Nederland steeds meer databanken gekoppeld, en iets moet wel een erg goed bewaard geheim zijn als het niet met een druk op de knop door elke ambtenaar is op te vragen. Hack-Tic zal regelmatig berichten over nieuwe vermommingen en plannen, en je door middel van 'in-depth' reportages altijd op de hoogte houden van de laatste ontwikkelingen.

De informatiemaatschappij wordt geregeerd door een klein clubje machtige heren op voetstukken, die van ver uit de hoogte doorgeven wat goed voor ons is. Zij bepalen namens het grote bedrijfsleven welke systemen er worden ingevoerd, zij bepalen welke gebruiken er wel en niet van de computer gemaakt worden. De buitenstaander wordt niet geacht mee te denken. Meedoen mag hij wel; "Koop maar een PC en een tekstverwerker en ga maar oefenen, aan typisten en typistes is nog behoefte genoeg. Als je braaf je best doet mag je volgende week gegevens intypen in een database."

Barstjes in het marmer

Hackers willen een geinformeerde maatschappij waarin mensen zelf kunnen beslissen welke informatie ze tot zich nemen. Een maatschappij zonder computercensuur. Maar als hackers in het nieuws kwamen stond steeds de techniek voorop. Hackers moesten rechtop zitten en het technisch wonderkind spelen. Kritische opmerkingen werden zo mogelijk wegggemoffeld achter het tradionele beeld van de hacker, en zodra de storm was gaan liggen waren de zaken weer zoals ze waren: een door onbenullen geregeerde vuilnisbelt waar niemand meer wijs uit wordt, hooguit een beetje beter beveiligd tegen 'onbevoegde inzage'.

Het werd dus tijd voor een eigen hacker geluid......

Hackers staan per definitie kritisch tegenover de informatiemaatschappij, al is het maar omdat die kritisch tegenover hen staat. Hackers komen echter nog te vaak over als strijders voor goede computerbeveiligingen. Ze worden maar al te vaak misbruikt als uithangbord voor bedrijven die systeembeveiliging aanbieden. Het is niet het doel van de hackgemeenschap om beter beveiligde computers te krijgen. We zien liever dat er goed gebruik wordt gemaakt van de techniek. Systemen die de privacy aantasten moeten niet beter beveiligd, ze horen niet te bestaan.

Nieuwe mogelijkheden

Het kan anders: computers kunnen worden gebruikt om mensen snel van informatie te voorzien. Ze kunnen grote

groepen mensen uit de hele wereld laten deelnemen in computer conferenties om zo kennis te nemen van andermans standpunt. Informatie over rampen kan sneller bekend worden, gegevens van wetenschappers kunnen sneller worden uitgewisseld. Mensen uit de hele wereld kunnen goedkoop en snel met elkaar corresponderen. Computernetwerken kunnen de menselijke samenleving vooruit helpen.

Van al deze prachtige mogelijkheden hoor je nu nog niets. Misschien geloof je er niet eens in. In onze artikelen zal regelmatig besproken worden hoe je met computernetwerken om moet gaan en hoe je zonder al te veel geld te besteden kunt beschikken over de informatie de je wilt hebben.

Wereldwijd

Hacken is internationaal. Grote databanken, informatiemonopolies en bestandskoppeling zijn dit ook. De wereld komt dichter bij elkaar en de tijd dat hackers elkaar internationaal niet nodig hadden is voorbij. Zie jij je al lopen in het Europa van 1992, met een ausweis op zak en een identificatiezender onder je auto? Gelukkig staan we niet alleen: ook in het buitenland zijn hackers actief. Met al deze organisaties (zoals de Chaos Computer Club in Hamburg) zal intensief worden samengewerkt zodat ook in 'das neue Europa' altijd een hack-geluid te horen zal zijn.

Het belangrijkste komt er in dit stukje bekaaid af. Rauwe HACK-INFORMATIE, daar zal Hack-Tic vol mee staan. Mensen met een technische interesse kunnen hun hart ophalen aan de vele technische truuks en tips. Alles voor de computerfanaten en de telefoonmaniakken. Soms verslagen van complete hacks met alle technische achtergrondinformatie, soms hints voor nog te plegen hacks. Hack-Tic stelt zich tot doel om alle ontwikkelingen op hackgebied in haar kolommen te hebben. Ook als de technische details je niet duidelijk zijn zul je in elk artikel de omvang en betekenis van een hack kunnen lezen. We hebben geen geheimen. Informatie is vrij!

Als je dit blad de moeite waard vindt kun je iets terug doen: maak jezelf abonnee. Ben je dat al, vertel het dan je vrienden/vriendinnen. We geven dit blad niet uit om er rijk aan te worden en voorlopig maken we er alleen maar verlies op. De prijs van Hack-Tic is laag omdat we hopen dat veel mensen behoefte hebben aan onze informatie. Treuzel dus niet en maak **35 gulden** over op bankrekening **98.72.84.541** en je krijgt 10 nummers lang het grootste, dikste, voordeligste, kleurrijkste en enige hackerblad van de Benelux in de bus.

'Hacking is a way of life' riepen verre voorouders al in de jaren zestig. Natuurlijk gaat Hack-Tic ook mee in de wereld van de hacker, een wonderlijke, open wereld vol eigen humor. Hacken is in ieder geval een kunstvorm die zeker niet is voorbehouden aan mensen die creatief met een computer om kunnen gaan. Ook op andere technische gebieden zijn hackers actief, en als je definities losjes hanteert is iedereen die zich verzet tegen de gevestigde orde, bestaande middelen creatief gebruikt en zich niet stoort aan regeltjes, een hacker.

Een tijdschrift beginnen heeft veel overeenkomsten met een geboorte: Zelfs in onze wereld vol computers en techniek is het nog maar de vraag of de baby levensvatbaar is. Al is deze baby nog niet zo zwaar, met haar grote mond denkt ze het nodige gewicht in de schaal te kunnen leggen.

PROOST

De Redaktie

kopij gezocht

We waarderen redaktionele bijdragen. Klachten over automatisering op de zaak? Schrijven! Informatie over nieuwe databanken? Schrijven! Nieuwe truuk ontdekt om leuke dingen te doen met de telefoon? Schrijven! Complete hack gepleegd? Schrijven! (en vergeet niet je log-files mee te sturen). Het hoeven geen hele artikelen te zijn, ook tips zijn soms goud waard. Natuurlijk hoeven we je naam niet te weten; What's in a name anyway?

Stuur je informatie naar:

Hack-Tic
Postbus 22953
1100 DL Amsterdam

telefax	**020-763706**
telex	**12969 neabs nl**
uucp	**..!mcvax!neabbs!rop**
fido	**2:280/1 Hack Tic**



As safe as the Bank of England!

Electronisch kluizensysteem diefstalgevoelig

Een geheel electronisch kluizensysteem is sinds enige tijd operationeel op het Amsterdamse Centraal Station. Dit systeem waakt dagelijks over de bagage van honderden reizigers. Er blijken echter de nodige truuks te zijn om dit systeem op te lichten. De mensen achter dit systeem blijken net zo betrouwbaar als hun apparatuur: ze weten dat er iets mis is, maar houden tegenover de reiziger vol dat het zijn eigen schuld is.

Een reportage van Herman Acker

Het lijkt zo handig: je stopt je bagage in een kluis en duwt de deur dicht. Vervolgens loop je naar de bij jouw sectie horende betaalterminal en betaalt fl. 1,50 (fl. 3,- voor de grotere kluizen). Het apparaat print dan vervolgens een bar-code kaartje (op een printertje uit het jaar nul: maakt een takkeherrie en doet er eeuwen over).

Met dit kaartje kun je het kluisje dan binnen 24 uur weer openen. Ben je te laat dan moet een boete worden betaald. Het kaartje werkt (zoals in het Nederlands is uitgelegd op de kluisdeur) maar 1 keer. Is de kluisdeur geopend dan stanst het apparaat een gaatje in de linker onderhoek van je kaartje om aan te geven dat dit kaartje al eens is gebruikt.

De altijd op het station rondhangende menigte van tasjesdieven en zakkenrollers heeft echter al een aantal methodes

ontwikkeld om de gebruikers van dit systeem van al die zware koffers te verlossen.

Truuk 1: Ik duw mijn kluis dicht en loop naar de terminal om te betalen. Een andere man staat daar voor zijn kluis te betalen (denk ik), dus ik wacht geduldig op mijn beurt. Als de man klaar is duwt een medeplichtige met z'n voet een ander kluisje in hetzelfde blok dicht. Ben ik aan de beurt dan betaal ik voor dit kluisje: leeg dus. Pas als ik terug kom en het lege kluisje openmaak zie ik dat het kluisnummer op mijn kaartje niet klopt. Maar dan is het al te laat.....

Truuk 2: Een stel stervensrijke Amerikanen staan te hannesen met hun bagage. "Nice city, Kopenhagen". "Shut up John, this is Amsterdam, give me that suitcase. Oh these stupid computers."

Op het toppunt van hun gehannes biedt een goed Engels sprekende heer zijn diensten aan. Hij weet wel hoe het systeem werkt. Je stopt je spullen er in en betaalt. Je krijgt dan een kaartje en dat kun je zo vaak gebruiken als je wilt om weer in je kluis te komen. Na 24 uur is het niet geldig. Hij raadt ze wel aan om het even te testen, want zeker weet je het met deze dingen nooit.

De vertrouwende Amerikanen gaan haast huilen van zoveel behulpzaamheid, stoppen snel hun spullen in de kluis en betalen voor de kaart. Daarna proberen ze hem nog even uit. Gerustgesteld dat alles in orde is streken ze hun kaart in de zak, duwen de kluis dicht en lopen weg.

De computer intussen denkt een stel nieuwe klanten te pakken te hebben en wil weer geld zien. Als binnen anderhalve minuut niet betaald wordt, opent het apparaat boos de kluis in kwestie en gaat weer digitale schaapjes tellen.

Truuk 3: Simpelere variant op truuk 1. Je duwt vlak voordat het slachtoffer zijn kluisje dichtdoet een ander kluisje dicht en laat het slachtoffer voor dat kluisje betalen. Nadat hij klaar is wacht het systeem anderhalve minuut en dan.... kloink!

Toen ik de geruchten over dit nieuwe systeem hoorde heb ik de proef maar eens op de som genomen. Ik heb een lege kluis gesloten en ben later die nacht teruggekomen om hem weer te openen. Ik deed alsof ik het slachtoffer was van truuk 1. "Help, ik stop mijn kaartje er in en het ding doet de verkeerde kluis open." Ik belandde via de bagagemedewerker van de NS ("Sja, dat is natuurlijk Uw eigen schuld. Neuh, daarvoor zijn wij niet aansprakelijk") uiteindelijk bij de spoorwegpolitie. De dienstdoende agent vertelde mij een aantal interessante details, waaronder de bovenstaande truuks, maar hij vertelde meer:

"De NS is het gedoe met die kluizen zat. Alle informatie over onregelmatigheden met die kluizen die wij hier inzamelen gaat naar de juridische afdeling van de NS. Die kunnen dat weer gebruiken voor een juridische procedure tegen de exploitant."

De juridische afdeling van de NS spreekt bij monde van Dhr. Dronker wel van een juridische procedure tegen de BEM (Bagagekluizen Exploitatie Maatschappij); "Maar dat die iets met de Amsterdamse stationskluizen te maken heeft is Uw eigen conclusie. In het belang van de NS en Servex kan ik over de procedure niets zeggen." (Servex is een volle NS-dochter die onder meer de afgifte van exploitatievergunningen voor stationskluizen regelt.)

En de BEM zelf? De in Roermond gevestigde firma laat haar telefoonlijn door een antwoordapparaat opnemen maar vergeet het bandje af te luisteren.

SPOORWEGPOLITIE
GEMEENTEPOLITIE AMSTERDAM
RECHERCHE

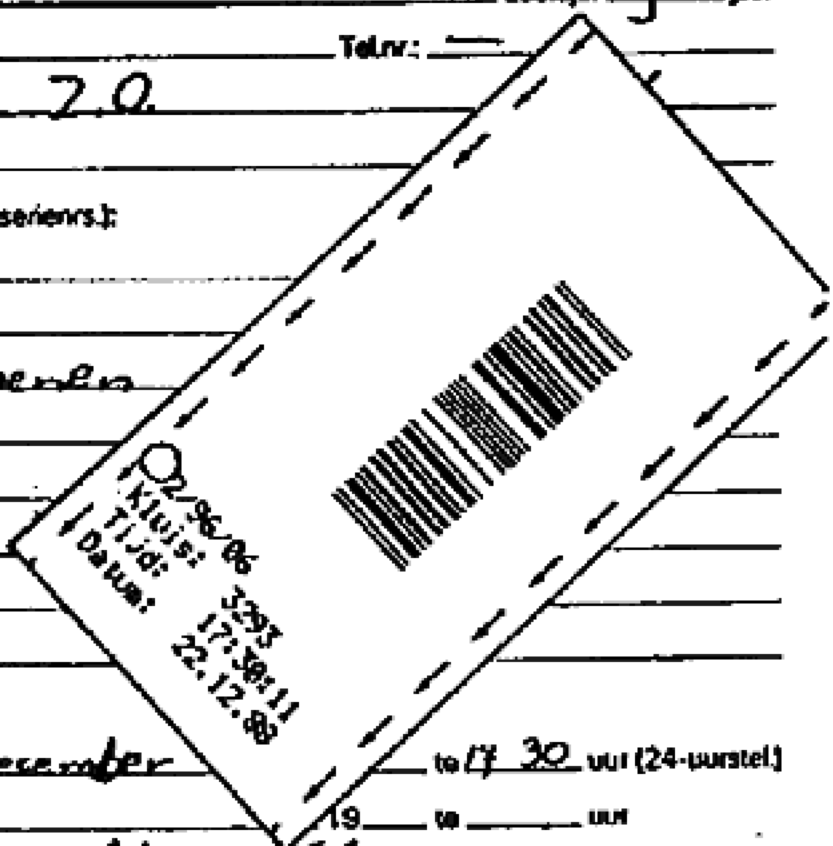
"Diefstal tas + inhoud."

AANGIFTE VAN DIEFSTAL
Pvb nr.: R
Jnd Pvo- /1988.

District: Noord-West.
Bureau: Stationsplein 21-25.
1012 AB Amsterdam.
Tel. nr.: 020-5578685.

Kopie, bestemd voor verzekeringsmaatschappij

Ik, ondergetekende,
Naam: Acker Leeftijd 19 jaar
Voornamen: Herman Tel.nr.: —
Woonplaats: 1102 AL A'dam Z.O.
Adres: Eekenstein 419
doe aangifte van diefstal van (voorwerp, eventueel serienrs.):
blauwe weekendtas
De inhoud is: slaapzak
1 paar gymschoenen



De diefstal is gepleegd op/tussen*:
(dag, datum): donderdag ; 22 december to 17 30 uur (24-uursstel.)
en (dag, datum): 19 te uur
op de (naam straat): afd. bagage A'dam CS te Amsterdam
ter hoogte van:
Deze diefstal is gepleegd op de volgende manier: ik sluit kluis maar vlak daarvoor werd andere kluis gesloten. Dit is niet door mij bemerkt, en toen ik terugkwam bleek ik voor een lege kluis betaald te hebben. Ik heb niet gezien wie de andere kluis heeft gesloten

De goederen behoren/het goed behoort* mij in eigendom toe. Aan niemand is toestemming gegeven tot het plegen van voornoemd feit.

Amsterdam, 23-12-88 19

Handtekening:

* doorhalen wat niet van toepassing is

xxx

Datumstempel:
22 *DEC 88
23 *DEC 88
SPOORWEGPOLITIE
STATIONSPLEIN 21-25
1012 AB AMSTERDAM

te Amsterdam 23 december 1988.
De agent Spoorwegpolitie, onbezoldigd adjudant Korps Rijkspolitie.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
De (Hoofd)agent van Gemeentepolitie te Amsterdam

Stamnr.: J. VISSER.
Dienstdoende: te Amsterdam.

OPLEIDING TOT TELECOMMUNIST

deel 1

In Amerika begon het al in de jaren zestig. Het door Bell (Amerikaanse PTT) aangelegde telefoonnet kon door middel van een tonensysteem om de tuin worden geleid. Er ontstond een sub-cultuur van 'phone-phreaks' (jargon: alle f's door de ph van 'phone' vervangen). Nu 'Ma Bell' veel centrale's vervangen heeft door onkraakbare types en op allerlei andere vormen van creatief telefoongebruik zware straffen heeft gezet is de cultuur aldaar een beetje aan het uitsterven. Hier in Europa, waar alles later komt, is phreaking nog een redelijk nieuw gegeven.

Door The Key en Peter Poelman

Het internationale telefoonnet lijkt misschien een tamelijk gesloten systeem. Maar als je wat vaker internationaal belt zul je gemerkt hebben dat aan het begin en eind van een internationaal gesprek vaak de vreemdste piepjes zitten.

Deze piepjes zijn de controlesignalen die heen en weer op de lijn gaan. Ze vertellen de centrale aan ontvangende kant met wie de beller kontakt wil en de opbellende centrale krijgt via het zelfde systeem van piepjes informatie over de voortgang van de gespreksopbouw. Als bijvoorbeeld de opbeller neerlegt en dus kennelijk niet langer prijs stelt op de verbinding wordt door middel van een piepje aangegeven dat de lijn weer vrij is.

En daar ligt het zwakke punt van dit type 'signaleringen': ze spelen zich geheel af binnen de audio-band. Dit wil zeggen dat alle gebruikte toontjes ook over de gewone 'customer'-lijn getransporteerd kunnen worden. Als ik een nummer in land X bel en dan het 'deze-lijn-is-weer-vrij piepje' op de lijn zet geeft mijn centrale dit gewoon door aan de 09 centrale. Deze let alleen op piepjes van de andere kant en geeft het piepje ook gewoon door. De inkomende centrale in land X stopt echter onmiddelijk met het opbouwen van het aangevraagde gesprek. Met een serie van nieuwe piepjes kan de centrale dan gevraagd worden een nieuwe verbinding op te bouwen (ook met nummers buiten land X).

Natuurlijk zijn de PTT's zich bewust van dit probleem, en nieuwe internationale lijnen signaleren dan ook niet meer binnen de spraakband, maar op frequenties die op gewone telefoonlijnen niet worden doorgegeven of door een nog nieuwer systeem met een gemeenschappelijk kanaal waarop alle signalering plaatsvindt.

De oude systemen zijn echter nog genoeg in gebruik om garant te staan voor jaren van jolijt en plezier. In dit artikel zullen we uitgebreid ingaan op het signaleringssysteem CCITT 4. Dit systeem is vooral op oude lijnen in Europa nog uitgebreid in gebruik. Het is beroemd geworden tijdens de 'Denemarken affaire', hobbyisten hadden toen een GRATIS 06 nummer gevonden dat doorschakelde naar een bedrijf in Denemarken. Zodoende kon men dus voor niets met de hele wereld bellen.

Het systeem werkt met toonreeksen, in principe opgebouwd uit 7 elementen.

Elementen

P	150 ms 2040+2400 Hz
X	100 ms 2040 Hz
Y	100 ms 2400 Hz

XX	350 ms 2040 Hz
YY	350 ms 2400 Hz
x	35 ms van 2040 Hz
y	35 ms van 2400 Hz

Toonreeksen

Van bellende naar ontvangende centrale:

Terminal seizure	PX
Transit seizure	PY
Clear forward	PXX
Forward transfer	PYY
Cijfer 1	yyyx
Cijfer 2	yyxy
Cijfer 3	yyxx
Cijfer 4	yxyy
Cijfer 5	yxyx
Cijfer 6	yxxy
Cijfer 7	yxxx
Cijfer 8	xyyy
Cijfer 9	xyyx
Cijfer 0	xyxy
Call operator code 11	xyxx
Call operator code 12	xxyy
Spare	xxyx
Incoming echo sup.	xxxy
ST end-of-pulsing	xxxx
Spare	yyyy

Van ontvangende naar bellende centrale

Term. proc.-to-send	X
Transit proc.-to-send	Y
Number received	P
Busy flash	PX
Answer	PY
Release guard	PYY
Blocking	PX
Unblocking	PYY

Gebruik

Deze tabellen zijn natuurlijk prachtig om te zien, maar wat doe je er mee. Allereerst moet je een methode hebben om deze toontjes te genereren. Hiervoor kun je een huiscomputer gebruiken mits die in staat is om twee tonen tegelijk te maken (dus geen IBM-PC of kloon).

Ben je zover, dan is de rest simpel: je maakt eerst een gesprek dat via een CCITT 4 (C4 is korter) lijn loopt. Als je genoeg ervaring met deze methode hebt kun je dat horen als een gesprek tot stand komt, maar voorlopig zul je het moeten hebben van erg veel proberen (misschien brengen we over een tijdje wel een cursus-cassette op de markt....)

Heb je eenmaal zo'n lijn gevonden (gratis, dan wel tegen een lagere prijs dan wat je eigenlijk voor het gewenste gesprek zou gaan betalen), dan geef je het 'Clear forward' signaal. Dit luistert een beetje nauw, dus je zult moeten experimenteren om het juiste moment te vinden (bijvoorbeeld na het tweede klikje op de lijn).

Op bepaalde lijnen hebben ze een grapje uitgehaald om dit onmogelijk te maken, in dit geval is de lijn na het geven van het 'Clear forward' signaal onmiddellijk in gesprek. Dan heb je pech gehad en zul je een andere lijn moeten proberen.

Als alles goed gaat hoor je een het 'Clear back' signaal. De andere kant heeft door middel van dit signaal bevestigd dat de lijn vrij is en is opgehouden met het tot stand brengen van het oorspronkelijk aangevraagde gesprek.

Je kunt nu twee dingen doen: je kunt een gesprek beginnen met een abonnee in het land waar ook de zojuist 'afgepiepte' centrale staat, of met een ander land. In het eerste geval benut je de centrale als eindstation en geef je het 'Terminal seizure' signaal. Wil je naar een ander land bellen dan geef je 'Transit seizure'.

Na 'Transit seizure' komt de centrale met een 'Transit proceed-to-send'. Nu kun je de landencode intoetsen met behulp van de cijfer-toonreeksen uit de tabel. Na het intikken van een cijfer geeft de centrale korte toontjes terug. Een 'y' betekent dat er nog meer cijfers nodig

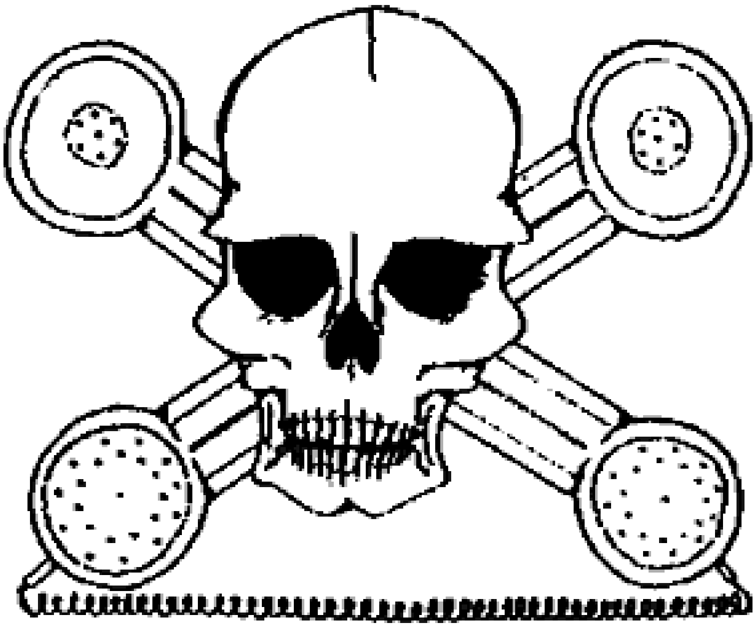
zijn, een 'x' (iets lager) wil zeggen dat er genoeg cijfers binnen zijn. Na het laatste cijfer even wachten. De volgende centrale in de keten komt dan of met een 'Terminal proceed-to-send' of met nog een 'transit proceed-to-send'. In het laatste geval moet je nog een keer het landnummer zenden, net zo lang tot je bij een centrale in dat land aankomt.

Nadat je een 'Terminal proceed-to-send' hebt ontvangen moet je eerst het gesprekstype aanduiden (z.g.n. 'discriminating digit'). Hiervoor kun je gewoon een nul nemen (andere digits zijn voor operatorgesprekken e.d.). Daarna komt het 'national significant number'. Dit is het telefoonnummer van de abonnee die je wilt spreken, zonder de eerste nul. Nu even wachten op verbinding en klaar is Uw kunstgebit.

Voor de gevorderden is deze truuk niet alleen bruikbaar om tegen gereduceerd tarief te bellen. Zij kunnen zich voordoen als operator en zo allerlei leuke gesprekken opbouwen, zelfs met landen die totaal niet automatisch bereikbaar zijn (zo neem je de overbelaste PTT medewerkers wat werk uit handen, laten we lief zijn voor elkaar).

Ook moet nog gezegd worden dat experimenteren met deze methode gratis is: de kosten gaan pas lopen op het moment dat er een verbinding tot stand komt (dus als er aan de andere kant iemand opneemt). Je betaalt altijd de kosten voor het oorspronkelijk gekozen nummer, ongeacht waar het gesprek uiteindelijk uitkomt. Dit betekent dat als ik een 06-0 nummer heb dat doorkiest over een C4 lijn, ik dan helemaal niks betaal, omdat mijn centrale denkt dat ik met een gratis nummer aan het bellen ben.

BEL GRATIS



THIS, The Hacker Information System

020 - 717666
(300,1200,2400,1200/75)

In een ver verleden waren er in Nederland maar een paar hackers. Nadat enkele hacks de krantekoppen hadden gehaald werden het er echter spoedig meer, en al gauw werd het hackerwereldje een tikje chaotisch. Het werd tijd voor een klein beetje ordening in de warrige telefonische geruchten- en berichtenstroom. Het idee voor THIS (The Hacker Information System) was geboren, een specifiek hacker BBS.

Er werd begonnen met THIS op een PC ergens in Rotterdam. Er was toen maar 1 telefoonlijn en 1 PC. Het BBS was echter drukbezet. Te drukbezet: de telefoon stond niet stil en het BBS was onbereikbaar. Toenmalig sysop Onno Tijdgat zocht contact met Max Keizer, sysop van NEABBS, ook toen al Nederlands grootste bulletin board, over de mogelijkheid om THIS onder te brengen als een sub-board in NEABBS.

Het idee was dat beide partijen daarmee beter af zouden zijn: THIS krijgt betere faciliteiten (nu: 16 lijnen, telex, fax en UUCP en fido netwerken) en NEABBS krijgt extra klanten.

Want hoewel begonnen uit zuiver hobbyisme is NEABBS uitgegroeid tot een volwassen bedrijf in BBS telecommunicatie. En hoeveel bewondering ik ook koester voor de vele sysops die hun BBS runnen zonder daarvoor geld aan hun gebruikers te vragen, ik betwijfel of er gratis BBS'en zijn die hun gebruikers kunnen bieden wat NEABBS heeft. Dit alles betekent echter wel dat je voor de toegang tot NEABBS moet betalen: 6 cent per minuut. Dit doe je door een zelf vast te stellen bedrag over te maken naar NEABBS.

Elke minuut dat je NEABBS gebruikt loopt je krediet dan af met 6 cent. Nader je de rode cijfers dan stuurt NEABBS je een herinneringsbericht zodat je nieuw geld kunt overmaken. Als je gebruik maakt van de speciale faciliteiten van NEABBS (telex, telefax, semafoonoproepen, UUCP usenet, FIDO Echomail etc.) wordt extra geld van je krediet afgetrokken.

Ik kan me goed voorstellen dat je denkt: "Tja luister eens: ik betaal genoeg voor mijn hobby; de computer is duur en de PTT is veel te duur. En dan zeker ook nog eens voor een BBS gaan betalen: ik kijk wel uit!" Het enige alternatief is echter een gratis BBS met beduidend minder faciliteiten en minder telefoonlijnen, zodat het lang niet altijd toegankelijk is.

Verder over THIS; terwijl het aantal files gestaag groeit, heeft THIS te maken met duidelijk ups en downs in de berichtensectie. De ene maand sterft het er van de berichten en lijkt het wel alsof er in de hele wereld geen veilige computer staat, de volgende maand worden er maar twee of drie berichten gepost.

Inmiddels zijn Peter Helders en ondergetekende co-sysops (schippers naast God) van Nederlands grootste hacker BBS, met enkele megabytes aan tekstfiles over de meest uiteenlopende onderwerpen. Het beleid van THIS (zeker als we het allebei druk hebben met andere dingen ontbreekt het nog wel eens aan beleid), is het er op gericht om THIS veelzijdig te houden en te proberen altijd over een gevarieerd aanbod in nieuwe tips en truuks te voorzien.

Een van de grote dilemma's in THIS is altijd: Hoeveel informatie geven we de beginner? Het is natuurlijk heel nobel om als groep 'gevorderde' hackers alle informatie beschikbaar te stellen, maar het is een beetje zuur als je met een pracht van een hack bezig bent en een goedbedoelende beginner maakt in zijn onwetendheid de systeembeheerder attent op de hack. Gevolg: weg hack.

Daarom is THIS verdeeld in niveau's. Nieuwe gebruikers van THIS komen na het aanvragen van toegang binnen op level B. Hier kunnen ze alleen maar de openbare berichten lezen en nog helemaal geen files downloaden. Zodra er een bijdrage aan THIS is geleverd (niet noodzakelijk hack-kennis, wel hack-betrokkenheid) wordt de gebruiker 'opgetrokken' naar level C.

Level D is voor de hacker die 'heeft laten zien wat hij kan' en level F tenslotte is voor een kleine groep van ingewijden. De oplettende lezer bemerkt hier dat level E ongebruikt is, maar het is altijd handig om een level over te hebben.

Het is natuurlijk onzin om alles in levels in te delen, en als voorstander van de 'free flow of information' vind ik dan ook dat alle informatie die geen betrekking heeft op nog in gang zijnde hacks vrij moet zijn voor iedereen die iets aan THIS bijdraagt.

ROP

In deze rubriek korte stukje informatie, of juist vragen om informatie. Antwoorden naar de redaktie postbus, telex, fax etc. etc. Nu staan hier een aantal vragen die ons zo snel te binnen schoten, de volgende keer zijn jullie aan de beurt.

Hacken onder Hoogspanning

Op het elektriciteitsnet staat lang niet alleen spanning die nodig is om allerlei handige apparaten zoals mijn computer te laten draaien. Via het net worden ook de nodige stuursignalen op de lijn gesuperponeerd. Een signaal met een veel hogere frequentie maar een kleinere amplitude wordt gebruikt om bepaalde zaken aan te sturen.

Ik woon zelf in de Zaanstreek en ik had laatst een elektraman over de vloer die mij van alles wist te vertellen over dit systeem. Zo zijn er tonen die straatverlichting aan en uit schakelen. Maar ook de dag- en nachttellers voor de industrie ('s nachts is stroom goedkoper) worden nu op deze manier bestuurd.

Ik riep natuurlijk onmiddellijk: "Ja maar, als ik zelf die tonen nou eens op het net zet vanaf het eerste het beste stopcontact?" Daar had de goede man geen antwoord op, maar de stilte die volgde sprak boekdelen.

Ikzelf heb helaas niet de nodige apparatuur en kennis om een en ander uit te zoeken. Wie maakt een apparaatje dat een nu-is-het-nacht-puls uitzendt zodra de nu-is-het-dag-puls is ontvangen?

Peter Poelman, Krommenie

Tele-Gambling

Ergens in Delft staat een leuk ding aan de telefoon. Je belt het en dan neemt het op met een pieptoon. Nu kun je vervolgens vijf cijfers intikken (op je DTMF telefoon), waarop een serie snelle piepjes volgt (alsof de code niet goed is).

Waarschijnlijk kun je allerlei leuke dingen doen als je de goede code weet, maar ja. Iedere poging kost vijftien cent, dus als je na 50.000 keer proberen beet hebt heeft dat jou (of je baas...) fl.7500,- gekost (pling, kassa).

Het leukste komt nog: als je dit nummer intikt op de 008 computer zegt het bok (draait onder VMS, vandaar) dat op dat nummer geen aansluiting zit. Waar moet het heen met de wereld als je niet meer op de PTT computer kunt vertrouwen voor je informatie...

Hier is ie: 015-783900, wie de code vindt krijgt een appeltaart.

John D. & The Key

Door schakelen wijs

De PTT levert doorschakelapparaten. Deze stammen nog uit de tijd dat doorschakelen niet in de centrale maar nog gewoon bij de abonnee thuis werd gedaan (op veel oude centrale's is dit nog steeds zo). Het nadeel is wel dat je twee telefoonlijnen nodig hebt.

Bel je op de uitgaande lijn van dit apparaat dan kun je met een speciaal piepertje instellen waar het ding naar doorschakelt. De toontjes die door dit piepertje gemaakt worden zijn geen DTMF toontjes, maar een soort riedeltjes.

Wie weet meer?

Eddie, your neighbourhood hacker

Wij zijn niet bang voor de tandarts.

Colgate mag dan, als we de reclame geloven, beschermen tegen gaatjes, maar de gaatjes in het wereldwijde computernetwerk van Colgate/Palmolive liegen er niet om.

Ik hoor echter al systeembeheerders zeggen dat hun systeem wel veilig is. Ik kan u verzekeren dat er geen veilige komputers bestaan en dat ze waarschijnlijk ook nooit zullen bestaan. Mocht er echter ooit een 100% veilige komputer komen dan is er nog steeds de menselijke schakel, die zoals we iedere keer weer merken, de zwakste schakel is in de beveiliging van een komputer.

Het computernetwerk van Colgate/Palmolive bestaat voor het overgrote deel uit computers van het merk Digital, type Vax, waarop in dit geval het VMS operating systeem draait. De computers waren met elkaar verbonden d.m.v. het zogenaamde Decnet. Dit netwerk maakt het mogelijk om over de hele wereld software, gegevens en post te verspreiden. Zo was het dus mogelijk om vanuit Luik (België) post te versturen naar bijvoorbeeld de vestiging in New York. Ook was het mogelijk om bijvoorbeeld als gebruiker van de vax in Luik, gebruik te maken van de vax in New York (waar misschien software en informatie is die voor bepaalde gebruikers over de hele wereld van belang kan zijn). Zo was het voor ons (een vriend die ook liever anoniem blijft en ik) heel makkelijk om van de ene computer over te springen naar de andere, zodat we op een gegeven moment bijna over de hele wereld binnen konden komen in vestigingen van Colgate/ Palmolive.

Het werd een obsessie om vanuit mijn woonplaats door te schakelen via België en Italië naar bijvoorbeeld Amerika, waar op dat moment computers die misschien wel tonnen kosten, bezig zijn om jouw data te verwerken. Het is nog leuker om te weten dat je evenveel privileges hebt als de eigenaar van die computer. Het enige wat hij meer kan, is de aloude stekker uit het stopkontakt trekken, wat hij niet zal doen zolang hij niets van jouw aanwezigheid heeft gemerkt. Doet hij het wel dan is hij nog weken, misschien wel maanden bezig om zijn systeem "optimaal" te beveiligen. Daarbij denk ik dan aan een operator die bij zijn baas op het matje wordt geroepen en gevraagd wordt of het systeem 'weer' veilig is, waarbij de operator (denkend aan vrouw, kinderen en de komende zomer op Mallorca) alleen maar positief kan antwoorden, terwijl hij zijn hart vasthoudt bij het weer koppelen van zijn systeem aan de buitenwereld (lees telefoon, datanet).

Toegang tot ....

Doormiddel van het langzaam opbouwen van de privileges kregen wij o.a. toegang tot project en financiele gegevens. Iets wat voor een groot bedrijf natuurlijk fataal kan zijn. Tevens konden we de post en telexberichten (deze liepen ook via de computer) van iedereen lezen, berichten over bereiding en verkoop van de produkten liepen dan over ons scherm. Nog interessanter waren de berichten van operators aan elkaar, zij vroegen elkaar om toegang op elkaars systeem, waarna er gelijk een bericht terugkwam met de login, het password en de mededeling dat de geadresseerde FULL-PRIVS kreeg op het systeem, waarna wij dus weer volledig toegang kregen tot een andere computer in het Colgate-netwerk. Zo drongen wij binnen in een

groot aantal computers van het Colgate concern.

De techniek.

Via via hebben wij op de vax in België (RNDLG) een login gekregen, zoals dat altijd gaat, een login met lage privileges, maar goed genoeg voor ons doel, want het enige wat wij nodig hebben is de gebruikerslijst en de nodelist. Nadat wij deze naar ons toe gehaald hadden zagen wij dat de gebruikerslijst een groot aantal potentieel kraakbare logins bevatte, en wonder boven wonder vond Colgate het ook nodig om zelfs een van deze logins full-privs te geven.

Nadat wij enigszins van deze stomme fout bijkwamen, en we in gedachten de systeembeheerder hartelijk bedankten vervolgden wij onze weg in het systeem. Uit ervaring was gebleken dat als we geen bewijs zouden hebben, Colgate ons nooit zou geloven als we dit vertelden, dus besloten we om overal, en uit elke node een logfile te gaan bijhouden (enkele fragmenten bijgevoegd).

We ontdekten zelfs met AUTHORIZE (een programma wat normaliter alleen door de systeembeheerder mag worden opgestart) dat de systeembeheerder zelf zijn password al ongeveer een jaar niet heeft veranderd, wat natuurlijk zoals je zult begrijpen erg stom is. Maar ok, dat is nog niets vergeleken met de andere fouten in het systeem.

Zo bleek het dus mogelijk om de verschillende files zoals de userlist en nodelist via de komputer in belgie van verschillende komputers over de hele wereld af te halen zonder dat wij daar een login hadden. Op deze manier vergaarden wij dus informatie over gebruikers van systemen, over de eventuele interessante info en over de netwerk mogelijkheden. Dit zou dus gewoonweg niet mogen, want in principe staat en valt je bedrijf met de computer, en op deze manier is het voor de concurrent heel simpel om de eventuele concurrentie van Colgate te peilen. Nog erger zou het zijn als er in dit geval veel persoonlijke gegevens zouden uitlekken, die in dit geval beperkt bleven tot de uitgaven aan salarissen en dat soort dingen. Toch is het een kwalijke zaak want wie weet wat er met uw informatie gebeurt in het bedrijf waar u werkt. Hoe wordt uw salaris bijgehouden?

Ik wil echter nog een ding zeggen tegen systeembeheerders, denk nooit dat uw systeem veilig is want misschien leest u volgende maand een artikel over uw systeem. "Never say never again".

Julius C. (1989) veni vidi hacki

[Uit de door de heer C. bijgevoegde stapel print-outs het volgende]

Een telex......

september 15, 1988

subject: pott competitive activity

for your information, please note that the uk company has identified a market research placement test of xxxx liquid in a 1 litre, handled bottle.

product description is: - 1 litre dishwasher cream

endorsements include:

"recommended by leading china manufacturers like xxx and yyy"

"xxxx is recommended for dishwashing machines, including hoover, indesit, and zanussi"

i bring this to your attention for the obvious reason of increased competitive activity within the region (further demonstrated by xxxx's recent expansion of xxx liquid add in switzerland). perhaps more of note is the focus and ability of yyy to secure such a wide range of manufacturers' endorsements -- an area we should continue to actively pursue.

please keep me advised of any/all competitive developments in your markets as

they relate to add's and, in turn, i will insure all operating units with a vested interest are kept informed.

regards, harry bluebell

[Omdat we vrezen dat Colgate/Palmolive betere advocaten heeft dan wij hebben we alle namen, kleuren etc. veranderd]

Een submenu......

502 FRINGE BENEFITS

```
********************************
50210 BONUS
50220 VACATION
50230 PAYROLL TAXES
50240 PENSION PLAN
50250 LIABILITY & GROUP
          INSURANCE
50260 LEAVING INDEMNITIES
50280 HOSPITALISATION
          INSURANCE
50290 TRANSPORT INDEMNITIES
50300 OTHER FRINGE BENEFITS
          (ticket-rest,..)
```

Een selectie uit de aangesloten systemen.

reactie Colgate

Natuurlijk is ook Colgate opgebeld voor een reactie, en die was voorspelbaar: "Ik heb het niet gedaan, daarvoor is XXX verantwoordelijk."

Na 2 uur bellen met diverse hotshots in Nederland en Belgie waren we 25 gulden armer en nog geen steek verder. De automatiseringschef voor de Benelux heeft volgens eigen zeggen met het VAX netwerk niets van doen (dit is al een hele vooruitgang: de rest van de automatiseerders moesten we eerst uitleggen wat een vax net is).

	Node	Links	Cost	Hops	Next Hop to Node			
1.32	RNDLG	0	0	0	(Local)	-	1.32	RNDLG
1.1	PARKAV	0	4	1	BNT-0	-	1.1	PARKAV
1.2	DCVAX1	0	4	1	BNT-0	-	1.2	DCVAX1
1.4	TCOP	0	4	1	BNT-0	-	1.4	TCOP
1.5	BADGE	0	4	1	BNT-0	-	1.5	BADGE
1.6	PSNAG1	0	4	1	BNT-0	-	1.6	PSNAG1
1.7	ARTHUR	0	4	1	BNT-0	-	1.7	ARTHUR
1.8	RCSNA1	0	4	1	BNT-0	-	1.8	RCSNA1
1.10	TCVAX1	0	4	1	BNT-0	-	1.10	TCVAX1
1.12	RNDRC2	0	4	1	BNT-0	-	1.15	TCVAX2

WORM OP HET INTERNET

Het internet verbindt een groot aantal research computers in de hele wereld. Een waanzinnig slimme programmeur heeft een programma ontwikkeld dat zichzelf razendsnel en zeer efficient over dit netwerk kan verspreiden.

Op het internet wordt ook nieuws over diverse onderwerpen over de aardbol gestuurd. De nieuwsgroep 'RISKS' (The risks of computing) bevatte vorig jaar november een groot aantal interessante berichten. (De hele structuur van de worm was al bekend toen de pers hier nog schreef dat 'men in het duister tastte'. Nu nog heeft de pers het over een virus in plaats van een worm. De artikelen spreken voor zich....

Hi Gang!

It's now 3:45 AM on Wednesday 3 November 1988. I'm tired, so don't believe everything that follows...

Apparently, there is a massive attack on Unix systems going on right now.

I have spoken to systems managers at several computers, on both the east & west coast, and I suspect this may be a system wide problem.

Symptom: hundreds or thousands of jobs start running on a Unix system bringing response to zero.

Systems attacked: Unix systems, 4.3BSD unix & variants (eg: SUNs) any sendmail compiled with debug has this problem. See below.

This virus is spreading very quickly over the Milnet. Within the past 4 hours, I have evidence that it has hit 10 sites across the country, both Arpanet and Milnet sites. I suspect that well over 50 sites have been hit. Most of these are "major" sites and gateways.

The bug in Sendmail:

When the Unix 4.3 BSD version of Sendmail is compiled with the Debug option, there's a hole in it.

Most Unix systems (BSD 4.3 and Suns) apparently do not have this bug. It exists only where the system manager recompiled Sendmail and enabled debugging.

This is bad news.

Date: Thu, 03 Nov 88 22:04:15 EST
Subject: A cure!!!!!

FLASH!!

Kevin ("Adb's your friend.") Braunsdorf just burst into my office with a cure discovered in the disassembled worm binary.

If there is an external variable in the library named "pleasequit" that is non-zero, the worm will die immediately after exiting. Thus, to kill any new worms, include a patch in your library that defines the symbol. The following shell file and source code will modify your C library to define this symbol.

It WON'T kill any currently linked and running versions, but it will prevent reinfection.

Subject: The Worm

Our site apparently didn't get hit, because our newly installed NSFnet router has been so flaky that it has been unusable. Just goes to show, I guess.

A REPORT ON THE INTERNET WORM
Bob Page
University of Lowell
Computer Science Department
November 7, 1988

Here's the scoop on the "Internet Worm". Actually it's not a virus - a virus

is a piece of code that adds itself to other programs, including operating systems. It cannot run independently, but rather requires that its "host" program be run to activate it. As such, it has a clear analog to biologic viruses -- those viruses are not considered live, but they invade host cells and take them over, making them produce new viruses.

A worm is a program that can run by itself and can propagate a fully working version of itself to other machines. As such, what was loosed on the Internet was clearly a worm.

The basic object of the worm is to get a shell on another machine so it can reproduce further. There are three ways it attacks: sendmail, fingerd, and rsh/rexec.

[hier volgt langdradige technische uitleg. Het komt er op neer dat de worm probeert om via het programma sendmail een opgestuurde C source te compileren (sendmail) en een sh op root bevoegdheid uit te voeren via een bug in 'fingerd'. Verder probeerde het systeem of er nog andere hosts op deze machine waren aangesloten, en zo ja dan werden ook deze geinfecteerd. Om hostnames uit user-directories te kunnen halen werden een groot aantal voor de hand liggende wachtwoorden geprobeerd (rsh/rexec).]

THE CRACKDOWN:

Three main 'swat' teams from Berkeley, MIT and Purdue found copies of the VAX code (the .o files had all the symbols intact with somewhat meaningful names) and disassembled it into about 3000 lines of C. The BSD development team poked fun at the code, even going so far to point out bugs in the code and supplying source patches for it! They have not released the actual source code, however, and refuse to do so. That could change - there are a number of people who want to see the code.

Portions of the code appear incomplete, as if the program development was not yet finished. For example, it knows the offset needed to break the BSD fingerd, but doesn't know the correct offset for Sun's fingerd (which causes it to dump core); it also doesn't erase its tracks as cleverly as it might; and so on.

The close scrutiny of the code also turned up comments on the programmer's style. Verbatim from someone at MIT:

"From disassembling the code, it looks like the programmer is really anally retentive about checking return codes, and, in addition, prefers to use array indexing instead of pointers to walk through arrays."

Anyone who looks at the binary will not see any embedded strings - they are XOR'ed with 81 (hex). That's how the shell commands are imbedded. The "obvious" passwords are stored with their high bit set.

Although it spreads very fast, it is somewhat slowed down by the fact that it drives the load average up on the machine - this is due to all the encryptions going on, and the large number of incoming worms from other machines.

[Initially, the fastest defense against the worm is is to create a directory called /usr/tmp/sh. The script that creates /usr/tmp/sh from one of the .o files checks to see if /usr/tmp/sh exists, but not to see if it's a directory. This fix is known as 'the condom'.]

NOW WHAT?

Most Internet systems running 4.3BSD or SunOS have installed the necessary patches to close the holes and have rejoined the Internet. As you would expect, there is a renewed interest in system/network security, finding and plugging holes, and speculation over what will happen to the worm's creator.

If you haven't read or watched the news, various log files have named the responsible person as Robert Morris Jr., a 23-year old doctoral student at Cornell. His father is head of the National Computer Security Center, the NSA's public effort in computer security, and has lectured widely on security aspects of UNIX.

Associates of the student claim the worm was a 'mistake' - that he intended to unleash it but it was not supposed to move so quickly or spread so much. His goal (from what I understand) was to have a program 'live' within the Internet. If the reports that he intended it to spread slowly are true, then it's possible that the bytes sent to ernie.berkeley.edu were intended to monitor the spread of the worm. Some news reports mentioned that he panicked when, via some "monitoring mechanism" he saw how fast it had propagated.

A source inside DEC reports that although the worm didn't make much progress there, it was sighted on several machines that wouldn't be on its normal propagation path, i.e. not gateways and not on the same subnet. These machines are not reachable from the outside. Morris was a summer intern at DEC in '87. He might have included names or addresses he remembered as targets for infesting hidden internal networks. Most of the DEC machines in question belong to the group he worked in.

The final word has not been written - I don't think the FBI have even met with this guy yet. It will be interesting to see what happens.

Article on the internet worm

AL FASOLDT is a technology writer (syndicated newspaper columnist) and audio writer (Fanfare Magazine), newspaper editor in Syracuse, NY (the daily Herald-Journal), poet, bicyclist, computerist who loves simple programming; a fan of the Atari ST and no fan at all of MS-DOS computers; 2 grown children.

"Let's start things off with some thoughts on who is really responsible here."

This is an article I wrote for distribution this coming week.

AThis can be reproduced in electronic form as long as the text is not altered and this note remains on top. Distributed by the Technofile BBS.

By Al Fasoldt

There's an untold story in the furor over the electronic virus that infected 6,000 mainframe computers across the country earlier this month.

Left out of the many accounts of the prank pulled by a Cornell graduate student is something that could be the single most important issue of computer networking in the next decade.

It is put most simply in the form of a question: Who is in charge of our mainframe computer networks?

In more complete terms, it can be stated this way: Are we placing too much trust in the systems managers who run our nation's medium- and large-size computer systems?

I am posing this question for a practical reason, not a theoretical one. Lost in the furor over the mass electronic break-in is the fact that it could have been prevented - if the people in charge of the computers had been doing their job.

The hacker, Robert Morris, exploited a weakness in the operating system of these computer systems. The weakness was known to the operating system's designers, and the company that supplies the operating system had long ago sent notices to all its customers explaining how to patch the operating system to fix the weakness.

All these thousands of systems managers had to do was read their mail.

Most of them didn't. Most of them ignored the plea from the operating system's designers to make the fix before someone broke into these computers through this weak area, called the "back door."

There is no other word for this than incompetence. Those who think it's unlikely that most mainframe computer systems managers are incompetent - at least in this one area, if in no other - have their heads in the sand.

Think of it in terms of human viruses. If doctors throughout the country were warned of a potentially dangerous weakness in a major drug and most of them did nothing about it, how forgiving would we be? We would demand that the medical profession act immediately to remove those doctors who don't have enough sense to protect the public.

Are we going to do the same thing in regard to our systems managers?

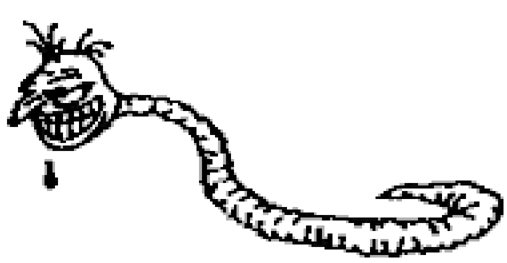
I'm a realist. I know what the answer is. They'll go on protecting their jobs by making up excuses. They'll tell the people who hired them that the entire subject is too technical to explain, but they have the situation well in hand.

Bull. Every systems manager who ignored the warnings on the flaws in Unix, the operating system that Robert Morris sailed right through, should be fired.

It's as simple as that. It's time that we treated networked computer systems seriously. It's time that we stopped accepting the technobabble from these incompetents as something that no one else can comprehend. The rest of us can comprehend it just fine, thank you.

If you agree, mail a copy of this column to your boss. Send a copy to the person who hires and fires the systems manager in your company or university. Send 'em a message before another Robert Morris sends them something else.

How can computers catch a virus? It's easy. Keep in mind that a computer works quite a bit like a human being. Both need a central processor to run properly - a CPU chip in one case and a brain and central nervous system in the other. And both need the correct programs to work right - an operating system in the computer and an autonomous set of instructions to the organs of the body in the human. Each one can get sick when a virus works its way into the system and throws it off stride. In both the computer and the human, the virus hides itself and alters the day-to-day operations of its host. In its mildest form, the virus merely slows everything down. The computer responds sluggishly, and the human feels weak and rundown. At its worst, the virus can make either type of host so sick that it may not recover without intensive care. So far, what we have been describing also characterizes a simpler form of intruder, called a worm. The difference between a worm and a virus is that worms don't create new copies of themselves, but viruses do; in fact, the strongest viruses in computers and humans can create new clones of themselves many times a minute. The major conceptual difference is that human viruses are actual creatures, and they can sometimes be seen under a microsope. But computer viruses are formless groups of numbers written as a program. This may make them seem less harmful than human viruses, but it would be a serious mistake for us to treat them that way.



CCC vandaag

Al vroeg in de tachtiger jaren waren de Duitse hackers georganiseerd in de CCC. De CCC, bekend van o.a. de grote NASA hack van vorig jaar en de uitgave van de Hacker-Bibel (inmiddels 2 delen verkrijgbaar) stond vooral bekend als een Hamburgse club. Hoewel dit in het begin van de jaren tachtig misschien ook zo was, is de werkelijkheid nu anders.

Hier in Nederland waren omstreeks 1985 slechts enkele mensen actief, en omdat zij geen club hadden opgezet is het hacken in die tijd tamelijk ontoegankelijk geweest. Nieuwe hackers konden alleen 'in de groep opgenomen worden' door tamelijk toevallige contacten met het groepje bekende hackers.

Is in Nederland de 'hackscene' (daarom) nog tamelijk klein, in Duitsland zijn honderden hackers actief. Als je dan ook de enorme afstanden binnen de Bondsrepubliek bekijkt is het niet meer dan logisch dat er zich kleinere regionale hackgroepen vormen.

De belangrijkste onderscheiden binnen de CCC op een rijtje:

Hoewel de CCC in **Berlijn** is ontstaan heeft het zwaartepunt altijd in Hamburg gelegen. De groep in Berlijn is nooit echt georganiseerd geweest: veel contact met de rest van de CCC is er niet, en in ieder geval manifesteert het Berlijnse deel van de CCC zich niet echt als groep.

Hamburg is van oudsher het middelpunt van de CCC wereld. Pas in het laatste jaar worden belangrijke zaken ook door niet-Hamburgers georganiseerd. De scene werd dan ook zo groot dat ze gewoon niet meer vanuit een punt te organiseren was. Steffen Wernery en Wau Holland (die nu in Heidelberg woont, daarover straks) hebben de bal hier aan het rollen gebracht, en het is niet meer dan logisch dat de 'macht' zich hier geconcentreerd had. Hoewel veel Hamburgse leden er nog steeds van overtuigd zijn dat Hamburg het magische centrum van de wereld is, lijkt de 'hacktop' aldaar het absoluut niet erg te vinden de macht aan de rest van de BRD over te dragen.

In **Lübeck**, tegen de Deense grens aan, manifesteert zich nu een nieuwe groep hackers. Deze hackers zijn goed georganiseerd en hebben duidelijke leiders. Hoewel de rest misschien terecht mort dat de Lübeckers 'Wehrmacht ähnlich' georganiseerd zijn, ze moeten ook toegeven dat je ze om een boodschap kunt sturen. Als je daar op een bijeenkomst komt, dan komen er ook 20 mensen, er is drinken, eten en slaapruimte, 'Alles in ordnung'.

In **München**, helemaal aan de andere kant van de Bondsrepubliek, zitten tussen de dijenkletsende Beieren een aantal uiterst pragmatische hackers. Waar in het noorden nogal eens grote problemen zijn rond zaken als het aannemen van geld van de media doet men hier niet moeilijk: de Münchenaren weten 'wat een mark waard is'. Wordt in de rest van het land toch in een underground-achtige omgeving gehackt, de zuiderlingen hebben alle meestal een nette baan. Desondanks kunnen ze soms hard-core uit de hoek komen met bijvoorbeeld harde dreigementen aan het adres van Philips in de tijd dat Steffen Wernery in Frankrijk in de gevangenis zat. Technisch wellicht op hetzelfde niveau als Hamburg, maar toch moeten we het geweten van de CCC elders zoeken.....

En wel in **Heidelberg:** hier zitten Bernd Fix en Wau Holland aan het hoofd van de wat oudere CCC'ers. Hier wordt niet gespeeld, hier wordt nagedacht over de toekomst van de informa-

tiemaatschappij. De werkelijk maatschappijkritische geluiden komen dan ook veelal uit Heidelberg. Ook de verbinding met de Duitse politiek ligt hier: de Duitse Grünen zijn door de Heidelbergers middels het rapport "Trau keinen computer den du nicht (er)tragen kannst" uitgebreid geadviseerd over computers, informatiemaatschappij en wat daar zoal verder bij komt kijken. In Heidelberg moet ook de echte hacker-ethiek gezocht worden: Brazil en Steven Levy kennen ze hier 'auswendig'.

In **Keulen** was al heel vroeg een groep met mailboxen en netwerken aan het spelen. Technisch is deze groep zeer goed, maar hiermee hadden ze al zo veel lol dat echte hacking hier nooit van de grond gekomen is. Deze groep heeft pas invloed gewonnen toen networking binnen de CCC belangrijker werd. Een van de mailboxen wordt door de Socialistische computerclub gerund.

Dan is er nog een vreemde eend in de bijt: in **Bielefeld** zit een groep computerkunstenaars die op een geheel alternatieve manier probeert iets met de computer te doen. Hebben met het hele modemgedoe weinig te doen, maar voelen zich in een groep alternatieve computergebruikers toch goed thuis.

Conflicten

Binnen de CCC zijn ook de nodige conflicten. Deze zijn echter niet zo zeer tussen de regio's als wel tussen de leden en de top van de CCC. (Misschien is het conflict met München over de te harde uitspraken in de pers een uitzondering). De leden verwijten de top te publiciteitsgeil te zijn en te veel in de openbaarheid te treden. De top verweert zich door te zeggen dat het nodig is bepaalde zaken steeds weer onder de aandacht van mensen te brengen. Ze zegt dat zij ook door veel leden zelf naar voren geschoven wordt omdat veel leden niet in de openbaarheid willen treden. Van de leden is vaak ook harde kritiek op Steffen Wernery te horen. Vooral toen hij probeerde zijn gevangenisverhaal uit Frankrijk aan de hoogste bieder te verkopen moest hij het zwaar ontgelden. Enige leden dreigden met opzeggen van hun lidmaatschap, maar het lijkt er op dat de zaak met een sisser is afgelopen.

Ook binnen de top van de CCC zijn spanningen. Een van de lastige kwesties is de ruzie rond Jürgen Wieckman. Jürgen is behalve hacker ook journalist en heeft meegewerkt aan 'Das Chaos Computer Buch'. Dit boek bevat behalve de geschiedenis van de CCC ook enige zeldzame kijkjes in de keuken, en dat is Jürgen niet onverdeeld in dank afgenomen.

Het is voor een Nederlandse hacker bepaald een schok om te zien hoe sommige hackers daar tegenover elkaar staan. Jürgen belt naar de organisatie van het congres; hij heeft een auto nodig om hem met zijn spullen naar het congres te vervoeren. Een van de aanwezige bestuursleden wordt gevraagd Jürgen op te halen. "Welke Jürgen?" vraagt hij. "Jürgen Wieckman". "Nee, die mag ik niet, sorry, dat doe ik niet."

Voordat ik december vorig jaar in Hamburg was dacht ik altijd dat het beter was als we ons in Nederland niet in een groep organiseerden, om dit soort problemen te voorkomen. Maar op het congres heb ik aan den lijve ondervonden hoe goed het is om iets van een organisatie te hebben. Samenkomsten kunnen gemakkelijker worden georganiseerd en de hacker-beweging is toegankelijker. Het bestaat niet langer alleen maar uit hele kleine bijeenkomsten bij mensen thuis, maar dan kunnen ook wat grotere dingen gedaan worden, zodat er meer mensen met hacken kennis kunnen maken.

ROP

CHAOS COMMUNICATION CONGRESS '88

28-30 december 1988

Ik had in Amsterdam al kennis gemaakt met enige leden van de Chaos Computer Club toen ze hier waren voor een info-show in Paradiso. Toen ik dus hoorde dat ze in Hamburg een congres organiseerden in de laatste week van december ben ik daar maar eens wezen kijken.....

De heenweg liftend afgelegd (met een laptop XT en een Canon X-07 handheld in mijn rugzak). 's Avonds laat kwam ik aan in Hamburg, waar ik met Steffen heb afgesproken, en bij hem slaap ik ook gedurende het congres. Voordat we naar zijn huis gaan laden we op de plaatselijke brandweerkazerne eerst nog even een oude brandweerwagen vol met telefoonspullen, luidsprekers en dergelijke. Steffen zit bij de brandweer, en dit mag hij lenen.

De volgende ochtend begint de voorbereiding voor het congres. Steffen en ik komen te laat aan bij het Eidelstätter Bürgerhaus: de hele club staat boos buiten te wachten omdat Steffen de sleutel heeft. Eenmaal binnen 'Geht's los'. Telefoonkabels worden aangelegd, computers geinstalleerd etc. etc. Ook wordt een perskamer ingericht waar mensen rustig kunnen werken aan artikelen over het congres. Men vraagt mij om bij de opening van het congres (woensdag) iets te vertellen over hacken in Nederland.

Aan het eind van de dag is een groot deel van de techniek in orde en keren we weer huiswaarts na eerst het Hamburgse uitgaansleven van dichtbij te hebben bewonderd.

De volgende ochtend blijkt het ineens middag te zijn. Ik wek Steffen en die blijkt maagkramp te hebben. Als we om 15.00 aankomen in het Bürgerhaus is er weinig veranderd. Men loopt een beetje in het rond maar lijkt zonder Steffen die de boel anders organiseert een beetje uit het lood geslagen.

Omdat er al maandag al zo veel gedaan is hoeft er vandaag niet veel te gebeuren. Dit leidt er toe dat een groot deel van de aanwezige hackers spelletjes (al dan niet op andermans computer) zit te spelen.

De laatste hand wordt gelegd aan het programma, het wordt duidelijk wat er zo al gaat gebeuren dit jaar. Hoewel: echt duidelijk wordt dat op een Chaos Congres nooit. Het programma is hier niet een star, statisch gegeven, maar een soort levend organisme: elke minuut verandert er wel iets en het hebben van een up-to-date print-out is een must.

Als woensdag het congres begint kom ik pas om 12.20 aan. Precies op tijd, ik kan gelijk het toneel op. Wau Holland opent het congres met een kort welkomstwoord en dan kom ik als eerste spreker. Ik had echter nog geen tijd gehad om mijn tekst te corrigeren, en ook voor een print-out had ik geen tijd. Dus daar zit ik met de laptop voor me, hakkelend in slecht Duits.

Als ik het heb over de gaten in autotelefoonnet 1 die in Duitsland nog ten volle benut kunnen worden kijkt men mij enigszins ongelovig aan. Pas later dringt het tot velen door dat de Duitse hackers hier inderdaad iets over het hoofd hebben gezien.

Duidelijk was echter dat de hackers hier niet geloven in een taalbarriere: ook al was je Duits erbarmelijk, men was men bereid rustig naar je te luisteren. Pas later realiseerde ik me dat dat natuurlijk ook kwam omdat ik mee hielp organiseren. Mensen die daar alleen maar als gast

kwamen hebben bepaald slechtere ervaringen met de toegankelijkheid van de organisatie (en een deel van de Duitse hackers).

Na de openingstoespraak begon de lol pas echt: in de hack-room werden adressen en NUA-lijsten uitgewisseld, PAD's opgebeld, computers gedemonstreerd en ga zo maar door. Grote groepen mensen om sommige computers, waar dan op dat moment iets spannends gebeurt.

In de andere ruimten vinden in de drie dagen dat het congres duurt allerlei conferenties plaats. Een greep uit het aanbod: UUCP, over het UUCP netwerk, PC-DES over het DES codeeralgoritme en een zeer snelle PC implementatie daarvan, geschreven door Bernd Fix, die ook de conferentie leidde. De leukste was eigenlijk "Dummheit in die Netzen". Onder deze ietwat sullige titel gaat een serieus probleem schuil: als je meer informatie krijgt moet je steeds selectiever zijn. Wat doe je als 90% van de informatie bestaat uit testberichtjes etc?

In de perskamer ondertussen probeerde men berichten over de loop van het congres de wereld in de krijgen. Een dataverbinding met DPA, het Duitse nationale persbureau, bewees goede diensten.

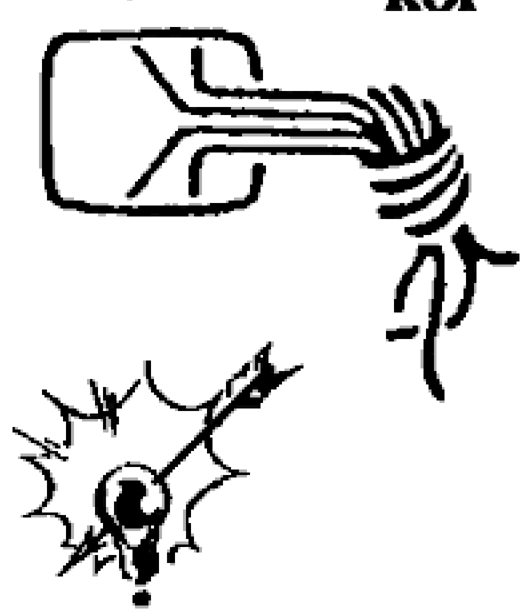
In de Markthalle, een zaal aan de andere kant van Hamburg, waren ook een aantal zaken georganiseerd die een grotere zaal nodig hadden. Zo was er woensdagavond het toneelstuk "Chaos im Computerclub", gespeeld door een toneelgezelschap dat niets met de CCC te maken had, maar hacken gewoon wel een spannend onderwerp vond. Hoewel het beslist niet onaardig was kun je niet zeggen dat de makers van dit stuk al te veel hinder hebben ondervonden van kennis van zaken op hack-gebied (gammele restjes acht-bitter die werden gepresenteerd als het nieuwste van het nieuwste en zo).

Donderdag vond er in die zelfde Markthalle een discussie plaats die het klapstuk van het congres had moeten worden: een confrontatie tussen Christian Lochte van de verfassungsschutz (bij ons BVD) en de CCC. Vooral over de criminalisering van de CCC in Duitsland waar de Verfassungsschutz hard aan meewerkt zou het nodige gezegd zijn.... Als Lochte gekomen was. Maar op het laatste moment werd telefonisch afgezegd om 'veiligheidsredenen'. Ook een telefoonverbinding was kennelijk voor de gezondheid van Lochte te gevaarlijk.

Bij gebrek aan tegenpartij is toen een discussie op gang gekomen over de gevaren van het nieuwe digitale telefoonnet ISDN, dat ook in Nederland in voorbereiding is. Met dit net kan veel makkelijker het bel-gedrag van mensen worden bekeken, zodat invoering van ISDN een inbreuk is op de privacy van telefoongebruikers.

Als het congres de volgende dag (vrijdag) wordt afgesloten lopen de meningen uiteen. Wie verwacht had een goed georganiseerd congres met een maximum aan informatie aan te treffen komt bedrogen uit. Wie uit was op een 'familietreffen' zat midden in de roos. Want door al die vervolgingen in Duitsland is de CCC een hechte vriendenclub geworden. Als je, zoals ik, het ontmoeten van leuke mensen ook belangrijk vindt dan is het Chaos Communication Congress '89 onmisbaar!

ROP



BACKUP

Ze zeggen wel eens dat hackers slechte mensen zijn die systemen stuk maken. Het tegendeel is waar: wij helpen de arme systeembeheerders door van belangrijke files in hun systeem een backup te maken. Mocht onverhoopt een hard-disk crash plaatsvinden dan kan de file eenvoudig uit het betreffende nummer van HACK-TIC worden overgetikt (systeembeheerders hoeven geen copyrightgelden af te dragen).
Een Hack-Tic lezersservice.

CONFIDENTIAL

Peter,

Theo's salary level and grade have so far been entirely a matter for you to specify from Holland; obviously any future arrangements will still have to be agreed by you. My engineering staff would recommend from what we have seen of Theo so far that he should be graded at the US equivalent of an TYRE CO2 position, Grade 8 on the University of Pittsburg scale. This is at the same grade as our more experienced technicians (three grades above our most recent hires) but two grades below our recently appointed electronics supervisor. If paid through the HUYT, Theo would therefore receive $24,696 per annum. If Anny were right (we do not think so), Theo would be at Grade 10 at a salary of $28,344 per annum. A compromise of grade 9 would yield a salary of $26,436 per annum, almost exactly what you paid him in 1986. (According to our records he was paid $18329.30 plus $7200 rent allowance plus $1064 medical insurance contribution, total $26,593 - slightly above our grade 9s). I would say that in view of the fact that Theo has tenure with you - whereas our grade 10s do not have tenure - that Theo's pay is already adequate to meet Anny's point of view, and that TRO can therefore expect him to work at this computer technician job, without any change in salary. This is a good job, involving training and the chance to develop his potential a great deal further. I would like, effective 1st July - when TRO takes over the management of Theo - that we manage Theo's career on the same operating basis as John Baker, and bill you in the same way as we bill you for John Baker's services. He would start at grade 9, with no initial change in salary (we would use the next cost of living increase due to HUYT employees to align things exactly). Unfortunately, there are obvious complications in that Theo's conditions of service here presently include provision of house rental etc., and his job, unlike John's is (I presume) tenured. The HUYT positions do not include all these privileges. I have asked Donald van Diepen to see if we could arrange to have Theo's superannuation contributions paid directly to Holland by the TYRE, and have all other aspects of his job managed through the HUYT. I would assume that the Dutch authorities would retain all Theo's rights of tenure if we were to make an arrangement like this. Comments?